IN THE CLAIMS

***Listing of the Claims***

1. (Currently Amended) A method that is implemented by a computer for reducing the occurrence of unauthorized use of on-line resources, comprising:

storing business rules for a plurality of companies having on-line resources;

receiving a message indicating a request from a user to use on-line resources;

identifying a company associated with the requested on-line resource from among the plurality of companies;

retrieving the stored business rules for the identified company;

determining whether the request requires authentication;

enabling the request to be fulfilled without authentication if the determination indicates that authentication is not required;

obtaining an indicia of physical identification from the user if the determination instead indicates that authentication is required;

comparing the obtained indicia to a stored indicia for the user; and

enabling the request to be fulfilled if the obtained indicia matches the stored indicia,

wherein the step of determining whether the request requires authentication includes determining whether stored business rules for the identified company associated with the requested on-line resource indicates that authentication for the user is required, and

wherein at least the determining and comparing steps are implemented by the computer.

2. (Previously presented) A method according to claim 1, wherein the step of determining whether the request requires authentication includes:

retrieving a stored profile containing the user's historical authentication patterns with respect to a plurality of network elements;

identifying certain network elements of the plurality of network elements in the stored profile as being associated with the requested on-line resource;

determining a score for the user based on the user's historical authentication patterns with the certain network elements; and

determining whether authentication is required for this request to use the on-line resource based on the score.

3. (Canceled)

4. (Previously presented) A method according to claim 1, wherein the step of determining whether the stored business rules requires authentication includes:

determining whether the user is listed by the company as always requiring authentication; and

requiring authentication if the user is listed.

5. (Previously presented) A method according to claim 1, wherein the step of determining whether the stored business rules requires authentication includes:

determining whether the user is listed by the company as never requiring authentication; and

not requiring authentication if the user is listed.

6. (Previously presented) A method according to claim 1, wherein the step of determining whether the stored business rules requires authentication includes:

determining whether the user is listed by the company as being completely denied access; and

completely denying access to the requested on-line resources if the user is listed.

7. (Original) A method according to claim 1, wherein the step of determining whether the request requires authentication includes determining whether the request is indicative of fraudulent behavior.

8. (Original) A method according to claim 7, wherein the fraudulent behavior is one or more of a collision violation, a velocity violation, and a customized trigger.

9. (Canceled)

10. (Previously presented) A method according to claim 1, further comprising:

determining whether the request is a card transaction;

determining whether restrictions applied to the user and an account associated with the request are satisfied by a purchase associated with the request; and

denying the request if the restrictions are not satisfied.

11. (Original) A method according to claim 10, wherein the restrictions are one or more of type of goods to be purchased, amount of purchase, time of purchase and location of purchase.

12. (Previously presented) A method according to claim 1, further comprising:

determining whether the request is an account transaction;

determining whether restrictions applied to an account associated with the account transaction are satisfied by the request; and

denying the request if the restrictions are not satisfied.

13. (Original) A method according to claim 12, wherein the restrictions are one or more of frequency of access and time of access.

14. (Previously presented) A method according to claim 1, further comprising:

determining whether the request is an account transaction;

determining whether use of the requested on-line resources are restricted for an account associated with the user; and

denying the request if the requested on-line resources are restricted for the account.

15. (Previously presented) A method according to claim 1, further comprising:

determining whether the request is a control transaction;

determining whether restrictions applied to the user associated with the control transaction are satisfied by the request; and

denying the request if the restrictions are not satisfied.

16. (Original) A method according to claim 15, wherein the restrictions are one or more of a parent control and an other control.

17. (Canceled)

18. (Previously presented) A method according to claim 1, wherein the indicia comprises a biometric that is one or more of a fingerprint, a voiceprint, a palmprint, an eye scan, and a handwriting sample.

19. (Previously presented) A method according to claim 1, further comprising providing access to the plurality of companies to allow them to configure their own individual set of stored business rules that are used in the determining step.

20. (Previously presented) An apparatus for reducing the occurrence of unauthorized use of on-line resources, comprising:

means for storing business rules for a plurality of companies having on-line resources;

means for receiving a message indicating a request from a user to use on-line resources;

means for identifying a company associated with the requested on-line resource from among the plurality of companies;

means for retrieving the stored business rules for the identified company;

means for determining whether the request requires authentication;

means for enabling the request to be fulfilled without authentication if the determination indicates that authentication is not required;

means for obtaining an indicia of physical identification from the user if the determination instead indicates that authentication is required;

means for comparing the obtained indicia to a stored indicia for the user; and

means for enabling the request if the obtained indicia matches the stored indicia,

wherein the means for determining whether the request requires authentication includes means for determining whether stored business rules for the identified company associated with the requested on-line resource indicates that authentication for the user is required.

21. (Previously presented) An apparatus according to claim 20, wherein the means for determining whether the request requires authentication includes:

means for retrieving a stored profile containing the user's historical authentication patterns with respect to a plurality of network elements;

means for identifying certain network elements of the plurality of network elements in the stored profile as being associated with the requested on-line resource;

means for determining a score for the user based on the user's historical authentication patterns with the certain network elements; and

means for determining whether authentication is required for this request to use the on-line resource based on the score.

22. (Canceled)

23. (Previously presented) An apparatus according to claim 20, wherein the means for determining whether the stored business rules requires authentication includes:

means for determining whether the user is listed by the company as always requiring authentication; and

means for requiring authentication if the user is listed.

24. (Previously presented) An apparatus according to claim 20, wherein the means for determining whether the stored business rules requires authentication includes:

means for determining whether the user is listed by the company as never requiring authentication; and

means for not requiring authentication if the user is listed.

25. (Previously presented) An apparatus according to claim 20, wherein the means for determining whether the stored business rules requires authentication includes:

means for determining whether the user is listed by the company as being completely denied access; and

means for completely denying access to the requested on-line resources if the user is listed.

26. (Original) An apparatus according to claim 20, wherein the means for determining whether the request requires authentication includes means for determining whether the request is indicative of fraudulent behavior.

27. (Original) An apparatus according to claim 26, wherein the fraudulent behavior is one or more of a collision violation, a velocity violation, and a customized trigger.

28. (Canceled)

29. (Previously presented) An apparatus according to claim 20, further comprising:

means for determining whether the request is a card transaction;

means for determining whether restrictions applied to the user and an account associated with the request are satisfied by a purchase associated with the request; and

means for denying the request if the restrictions are not satisfied.

30. (Original) An apparatus according to claim 29, wherein the restrictions are one or more of type of goods to be purchased, amount of purchase, time of purchase and location of purchase.

31. (Previously presented) An apparatus according to claim 20, further comprising:

means for determining whether the request is an account transaction;

means for determining whether restrictions applied to an account associated with the account transaction are satisfied by the request; and

means for denying the request if the restrictions are not satisfied.

32. (Original) An apparatus according to claim 31, wherein the restrictions are one or more of frequency of access and time of access.

33. (Previously presented) An apparatus according to claim 20, further comprising:

means for determining whether the request is an account transaction;

means for determining whether use of the requested on-line resources are restricted for an account associated with the user; and

means for denying the request if the requested on-line resources are restricted for the account.

34. (Previously presented) An apparatus according to claim 20, further comprising:

means for determining whether the request is a control transaction;

means for determining whether restrictions applied to the user associated with the control transaction are satisfied by the request; and

means for denying the request if the restrictions are not satisfied.

35. (Original) An apparatus according to claim 34, wherein the restrictions are one or more of a parent control and an other control.

36. (Canceled)

37. (Previously presented) An apparatus according to claim 35, wherein the indicia comprises a biometric that is one or more of a fingerprint, a voiceprint, a palmprint, an eye scan, and a handwriting sample.

38. (Previously presented) An apparatus according to claim 20, further comprising means for providing access to the plurality of companies to allow them to configure their own individual set of stored business rules that are used by the determining.

39. (Previously presented) An apparatus for reducing the occurrence of unauthorized use of on-line resources, comprising:

a server that is adapted to communicate with a network based service so as to receive a message indicating a request from a user to use the network based service;

a rules subsystem coupled to the server that determines whether the request requires authentication, the rules subsystem causing the server to enable the request to be fulfilled without authentication if the determination indicates that authentication is not required and causes the server to obtain an indicia of physical identification from the user if the rules subsystem instead determines that authentication is required; and

a business rules database coupled to the rules subsystem, the database storing business rules for a plurality of companies having on-line resources;

an authentication subsystem coupled to the server that compares the obtained indicia to a stored indicia for the user,

wherein the rules subsystem is adapted to identify a company associated with the requested on-line resource from among the plurality of companies, retrieve the stored business rules for the identified company from the business rules database and determine whether the stored business rules for the identified company associated with the requested on-line resource requires authentication for the user, and

wherein the server sends a signal to the network based service that the request is to be fulfilled if the authentication subsystem determines that the obtained indicia matches the stored indicia.

40. (Previously presented) An apparatus according to claim 39, further comprising:

a profile database coupled to the rules subsystem, the profile database maintaining a stored profile containing the user's historical authentication patterns with respect to a plurality of network elements,

wherein the rules subsystem is adapted to retrieve the user's stored profile from the profile database in response to the request, identify certain network elements of the plurality of network elements in the stored profile as being associated with the requested on-line resource, determine a score for the user based on the user's historical authentication patterns with the certain network elements, and to determine whether authentication is required for the user for this request to use the on-line resource based on the score.

41-42. (Canceled)

43. (Previously Presented) An apparatus according to claim 39, further comprising a user profile subsystem coupled to the server which is adapted to determine whether the request is indicative of fraudulent behavior, wherein the fraudulent behavior is one or more of a collision violation, a velocity violation, and a customized trigger.

44. (Canceled)

45. (Previously presented) An apparatus according to claim 39, wherein the indicia is a biometric, the apparatus further comprising a biometrics database that stores a plurality of biometrics for a respective plurality of users, and wherein the plurality of biometrics includes one or more of a fingerprint, a voiceprint, a palmprint, an eye scan, and a handwriting sample.

46. (Previously Presented) A method according to claim 2, wherein the step of determining the score includes:

applying a weight to each of the certain network elements based on a relative importance of the certain network elements;

evaluating the user's historical relationship with each of the certain network elements; and

aggregating the score using the weighted evaluations.

47. (Previously Presented) A method according to claim 46, further comprising:
allowing a system administrator to configure the respective weights for the plurality of network elements.

48. (Previously Presented) An apparatus according to claim 21, wherein the means for determining the score includes:

means applying a weight to each of the certain network elements based on a relative importance of the certain network elements;

means evaluating the user's historical relationship with each of the certain network elements; and

means for aggregating the score using the weighted evaluations.

49. (Previously Presented) An apparatus according to claim 48, further comprising:

means for allowing a system administrator to configure the respective weights for the plurality of network elements.

50. (Previously presented) An apparatus according to claim 39, wherein the rules subsystem is further adapted to apply a weight to each of the certain network elements based on a relative importance of the certain network elements, evaluate the user's historical relationship with each of the certain network elements, and aggregate the score using the weighted evaluations.

51. (Previously Presented) An apparatus according to claim 50, further comprising:
an administrator service that allows a system administrator to configure the respective weights for the plurality of network elements.